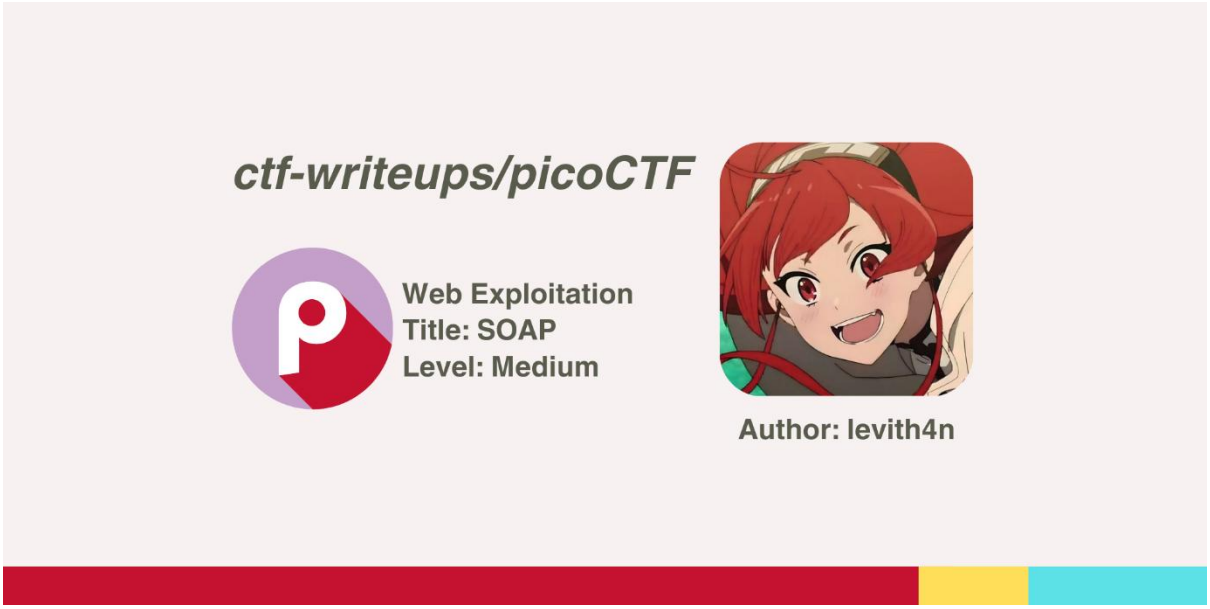
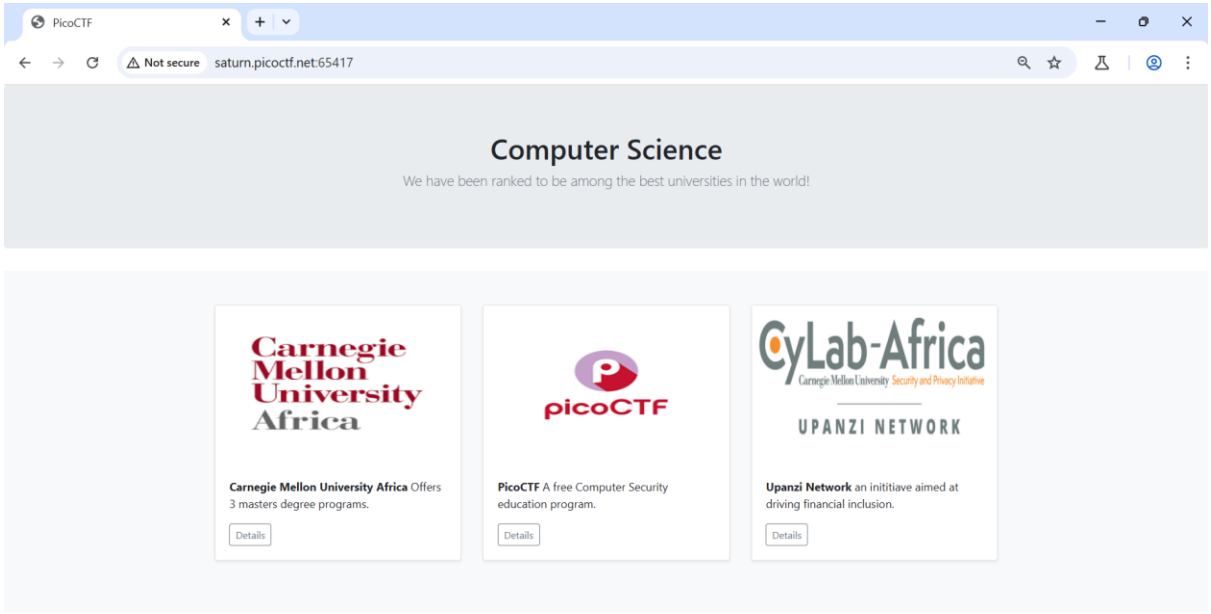


Description

Author: Geoffrey Njogu

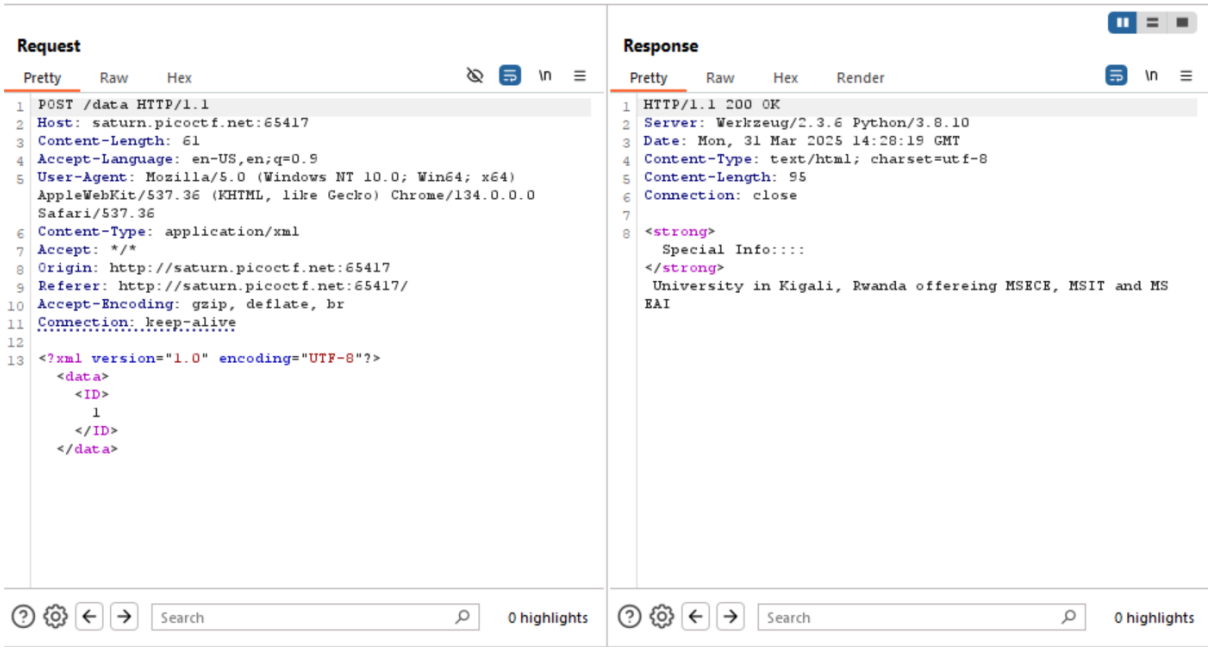
The web project was rushed and no security assessment was done. Can you read the /etc/passwd file?
Hints 1: XML external entity Injection

Ini adalah tampilan dari aplikasi web yang akan kita uji, terdapat tiga fitur yang sepertinya digunakan untuk menampilkan tentang suatu detail.

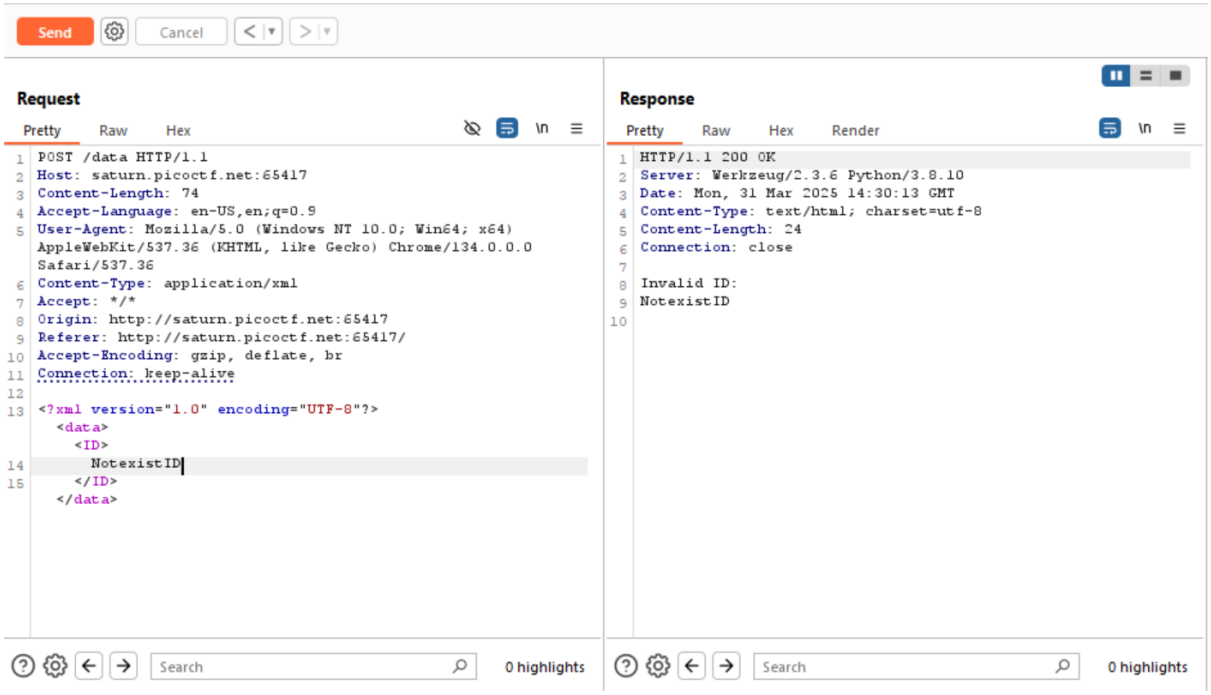


Pertama, saya langsung mencoba melakukan intercept menggunakan burp intercept pada salah satu fitur tersebut dan menemukan bahwa request HTTP dikirim dalam format XML, pada umumnya ini adalah XML-based API seperti SOAP, walaupun tidak semua XML-based API menggunakan SOAP.

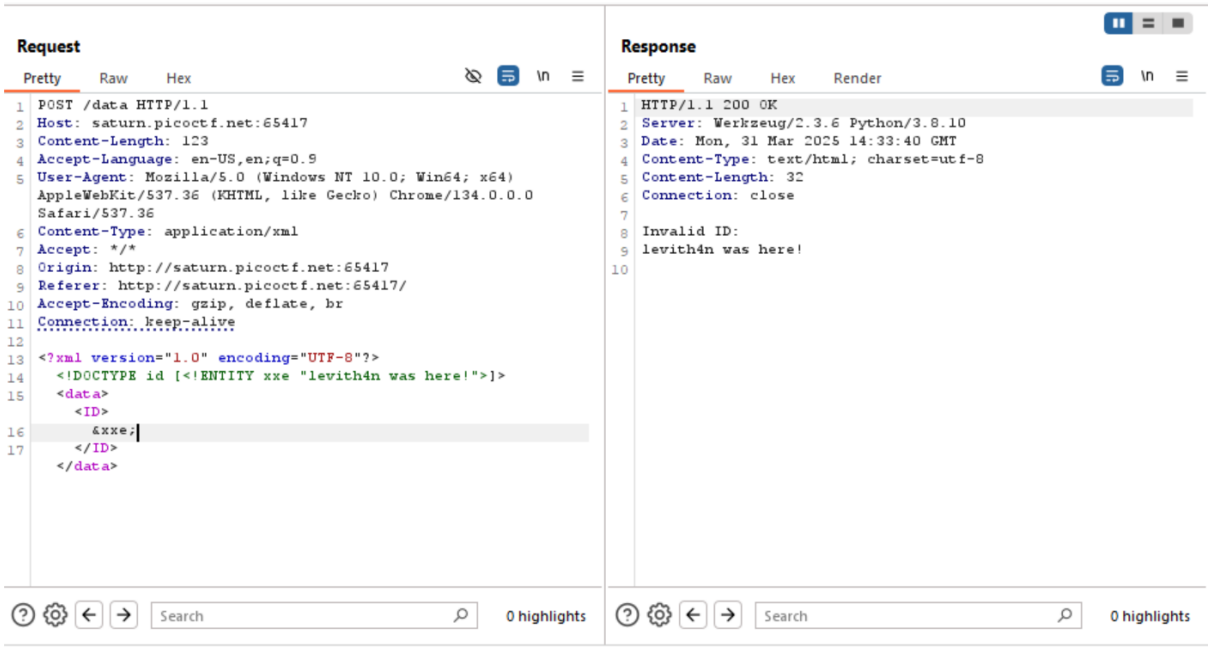
Setelah itu, saya langsung memindahkan traffic tersebut ke burp repeater guna melihat response dalam keadaan normal.



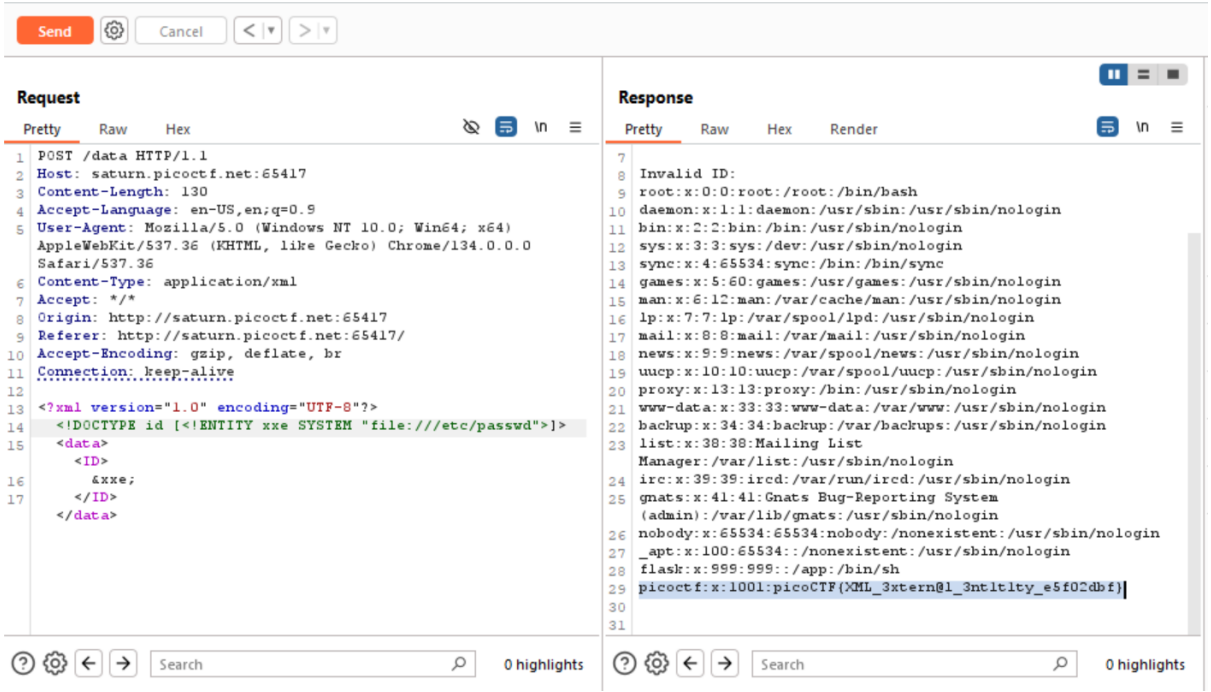
Kemudian, saya mencoba untuk mengganti nilai ID menjadi ‘NotexistID’ guna melihat response saat dalam keadaan error. Ternyata, saat dalam keadaan error, aplikasi web akan menampilkan pesan ‘Invalid ID’, diikuti dengan ID yang tidak valid tersebut. Tentu saja hal ini dapat saya coba manfaatkan untuk menyisipkan *internal entity*.



Saya mencoba menyisipkan *internal entity* dalam *DTD Internal* guna mengecek apakah XML Parser mengizinkan penggunaan custom DTD. Saat entity dipanggil pada dokumen XML, strings “levith4n was here” ditampilkan pada response, sehingga hal ini dapat dimanfaatkan untuk eksploitasi.



Terakhir, saya mencoba mengeksploitasi dengan medefinisikan *external entitiy* yang mengakses file sensitif seperti ‘file:///etc/passwd’, kemudian saya mencoba mereferensikanya dan berhasil memperoleh flag melalu isi file tersebut.



Thank you for reading!